UNIVERSIDAD SIGLO 21

TRABAJO FINAL DE GRADO

PHISHING Y PHARMING

"La problemática de la determinación de competencia en casos extraterritoriales."

PROYECTO DE INVESTIGACION APLICADA

ABOGACIA

BERMUDEZ LUCIANO JOAQUIN

DNI 37.466.108

VABG 26112

2019

Resumen

La evolución tecnológica trajo consigo inmensos cambios en la cotidianeidad de las personas, incluyendo la interrelación de las personas y sus bienes. Las Tecnologías de Información y Telecomunicaciones crearon además de progreso, una vulnerabilidad importante a sus usuarios debido al nacimiento del "ciberespacio", un mundo virtual que hace sencillo el contacto de los individuos con potenciales criminales.

Poniendo especial atención en el "ciberespacio" y su extensión característica que sobrepasa los límites jurisdiccionales de las distintas naciones del mundo, se podrá comprender los grandes inconvenientes que le ha causado a los sistemas legales existentes basados en fronteras físicas; provocando un gran problema de aplicación de las legislaciones a estos delitos llevados a cabo en distintas jurisdicciones.

Éste trabajo en particular analizará los delitos denominados "Phishing" y "Pharming" haciendo un enfoque especial en sus características y en los obstáculos con los que se encuentran los ordenamientos jurídicos a la hora de determinar la competencia de los juzgados que tendrán a cargo la dificultosa tarea de perseguir y juzgar a los actores de estos actos negativos, que actualmente están en constante aumento en cuanto a su cantidad y especialidad en su medio comisivo.

Palabras clave: Cibercrimen - Competencia - Jurisdicción - Phishing – Pharming.

Abstract

The technological evolution brought with it immense changes in the daily life of people, including the interrelation of people and their goods. The Information and Telecommunications Technologies also created progress, an important vulnerability to its users due to the birth of "cyberspace", a virtual world that makes the contact of individuals with potential criminals easy.

Paying special attention to "cyberspace" and its characteristic extension that exceeds the jurisdictional limits of the different nations of the world, it will be possible to understand the great inconveniences it has caused to existing legal systems based on physical borders; causing a great problem of application of the legislations to these crimes carried out in different jurisdictions.

This particular work will analyze the so-called "Phishing" and "Pharming" crimes, making a special focus on their characteristics and the obstacles that legal systems face when determining the jurisdiction of the courts that will be responsible for the difficult task of prosecuting and judging the actors of these negative acts, which are currently constantly increasing in terms of their quantity and specialty in their media.

Keywords: Cybercrime - Competition - Jurisdiction - Phishing - Pharming.

"Los criminales en vida real también lo serán en internet, donde la policía necesita ser un poco más sofisticada. El crimen online es sólo parte de la maduración del medio"

Bill Gates, Massachusetts Institute of Technology. (1996)

AGRADECIMIENTOS

Agradezco a mi incondicional sostén, a mis grandes guías y a mi mayor orgullo que son mis padres, Patricio y Silvina. Tuve la suerte de nacer con el mayor regalo que me otorgó la vida, que conllevó un par de años más terminar de abrirlo, que son mis hermanos: Pablo, Fernanda, Belén y Valentina. Es a ellos y a mis padres a quienes dedico esto, que al fin y al cabo es a quienes también les pertenece por todo lo que han hecho por mí.

También agradezco a mis amigos, que supieron entenderme en aquellos momentos importantes en los que no pude estar presente, y me dieron la mano para poder sortear toda piedra que se interpusiera en mi camino.

A mis abuelos, que siempre me han abierto las puertas para brindarme un segundo hogar, y a los que desde el cielo protegen y guían mi destino.

Por último, pero no menos importante, a mi madrina, quien me acompañó en los primeros pasos de la apasionante carrera del derecho.

Agradezco a todas las personas que han invertido en mí, cariñosa y desinteresadamente, su tiempo; y aprovecho esta oportunidad para manifestarles mi imposible arrepentimiento de haber compartido, con cada uno de ustedes, los imborrables momentos que este camino ha dejado y que hoy se convierte en un final repleto de comienzos.

¡Gracias!

ÍNDICE

Introducción

El Phishing y el Pharming son los nuevos crímenes mejor organizados de nuestro siglo, donde el estafador engaña a los usuarios para hacerse con información confidencial y personal. Por su lado el Phishing utiliza la ingeniería social, donde se utilizan correos fraudulentos para llevar a los internautas desprevenidos a sitios web falsos.

El Pharming es por su parte, una forma de Phishing mejorada debido a que se aprovecha de códigos maliciosos para llevar a cabo ataques sofisticados.

Una vez utilizadas estas modalidades fraudulentas, los estafadores proceden a utilizar los datos para sus intereses, los cuales son mayormente patrimoniales, creando un grave perjuicio para las víctimas.

Estos medios de comisión de delitos, pueden llevarse a cabo en diferentes territorios, por lo que éste trabajo de investigación tiene como objetivo general llegar a la respuesta de quien es competente en los casos donde el autor, las víctimas y/o el destino del patrimonio afectado se encuentran en diferentes territorios, por ende con una sobre posición de jurisdicciones y legislaciones.

La delimitación temporal de este trabajo en el campo del derecho, partirá desde la aprobación de la ley Nº 26.388 en el año 2008, Luego se avanzará cronológicamente hasta llegar al año 2017, en el cual entra en vigencia la ley Nº 27.411 mediante la cual Argentina comenzó a formar parte del Convenio de Budapest sobre Ciberdelitos. Durante y con posterioridad a los momentos mencionados, se rastrearán instrumentos acordes al tema de investigación hasta llegar a la actualidad.

Éste trabajo final fija como hipótesis a comprobar, que a partir del principio de territorialidad[1] y de ubicuidad previstos en nuestro Código Penal y en nuestra Constitución Nacional, los órganos encargados de estos hechos delictivos son principalmente los tribunales federales o los locales de aquellos lugares donde fue cometido la mayor parte de la acción o en su defecto, donde se produjo el resultado.

[1] Art. 1 del Código Penal Argentino.

Se dispondrá del tipo de investigación exploratorio ya que es útil para tener mayor conocimiento y precisión sobre el objeto de estudio. (Yuni J. y Urbano C., 2014) De forma complementaria, se utilizará el tipo descriptivo para llevar a cabo la descripción de las características del fenómeno en cuestión; debido a que permitirá, mediante la recolección de diferentes conceptos, precisar las características del proceso al que hacemos énfasis. (R. Hernández Sampieri, C. Fernández-. Collado y P. Baptista Lucio, 2006)

Éste Trabajo Final de Grado se compondrá de tres capítulos. El primero se desarrollará en base a las nociones básicas del tema, empezando por explicar los fenómenos llamados "ciberdelitos", las características que poseen, y la clasificación dada por órganos internacionales.

El segundo capítulo especificará el tipo penal que se ha elegido como objeto de estudio, desarrollando su etimología, sus antecedentes, los sujetos partes y el bien jurídico protegido.

Por su parte, el tercer capítulo estudiará la competencia establecida en nuestro ordenamiento, conceptualizando la jurisdicción y la competencia en sus diferentes modos, para finalmente exponer casos jurisprudenciales que demuestren la interpretación casuística de los delitos informáticos y las respectivas soluciones brindadas a los casos de competencia negativa.

CAPITULO I

NOCIONES BÁSICAS

Introducción

El inicio de este trabajo comenzará con el desarrollo de las nociones básicas para el conocimiento del tema a abordar. El primer capítulo tendrá como fin la clarificación de las ideas conceptuales sobre los delitos informáticos en forma general, en los cuales encontramos diferentes autores que no consiguen acordar, valga la redundancia, conceptos que puedan abarcarlos para poder definir de forma universal a estos fenómenos, como así también a las características que contienen.

Se hará mención sobre la falta de regulación específica por parte del ordenamiento jurídico argentino, lo cual provoca variados inconvenientes a la hora de enmarcarlos en los delitos tradicionales que ya se encontraban en él.

Posteriormente, se desarrollarán conceptos básicos del derecho penal para dejar en evidencia la importancia de la tipificación de los delitos para poder iniciar los mecanismos procesales para la investigación y sanción de conductas lesivas a los bienes jurídicos protegidos de las personas.

Por otro lado se definirán las características especiales que este tipo de delitos ostentan, diferenciándose ampliamente con los delitos tradicionales, cuyas diferencias hacen evidente la necesidad que ha provocado en los distintos campos jurídicos del mundo de modificar e innovar en sus normas, para poder combatirlos de una manera eficiente, por lo que se han establecido distintos convenios internacionales en su nombre.

Para finalizar, se expondrán las clasificaciones que tanto la Organización de las Naciones Unidas, como el Convenio de Cibercriminalidad, llevado a cabo en el año 2001 en la ciudad de Budapest, les han otorgado con el objeto de prevenirlos como así también de promover la cooperación internacional en la persecución e investigación de estos hechos delictivos.

1.1 Delitos informáticos

Para comenzar es importante destacar que si bien gran variedad de autores han definido estos fenómenos, la doctrina aún no ha podido llegar a un consenso sobre el concepto universal de los delitos informáticos. Tampoco hay un acuerdo en distinguir especialmente estos delitos con los tradicionales, ya que varios autores sostienen que son equivalentes a estos últimos, diferenciándose únicamente en el medio empleado para realizarlos.

En nuestra nación, por ejemplo, aun las normas no lo han conceptualizado expresamente; y es razonable en el sentido de que el derecho argentino es relativamente un recién iniciado en éste ámbito, aunque este tipo de conductas lesivas a personas y bienes jurídicamente protegidos datan de aproximadamente tres décadas, partiendo de los primeros casos de la utilización de la informática como medio comisivo de actos lesivos en el mundo, de los que al menos se tiene noción.

Ante la variedad de conceptos de la que se ha hecho mención, tomaremos el del Dr. Julio Téllez Valdés (2008), ya que realiza una diferenciación de la forma típica y atípica que nos servirá para comprender la importancia de la incorporación de los delitos dentro del ordenamiento jurídico. Según este autor, los delitos informáticos atípicos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin". En cambio, los típicos son aquellas "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (p. 188).

Ésta última definición es la que se vincularía con la función punitiva del derecho penal, debido a que, según la teoría general del delito, una conducta para considerarse como tal requiere que sea una acción típica, antijurídica y culpable, lo cual se explicará brevemente a continuación. Según la teoría mencionada, el delito tiene los siguientes elementos constitutivos, cuyos conceptos construiremos con la ayuda del Dr. Carlos Lascano (2005):

- *Acción*: puede manifestarse de dos formas, como acción u omisión. En el primero de los casos el individuo realiza una conducta prohibida por la norma, a diferencia de la segunda modalidad, donde lo que sucede es una desobediencia a la orden de una norma en los casos que las circunstancias ameriten llevar a cabo una determinada acción, la

persona esté en condiciones de realizarla y ésta evite hacerlo.

- *Tipicidad*: se logra con la descripción abstracta y taxativa de los diferentes comportamientos prohibidos por la ley, llevada a cabo por el legislador, como así también de la estipulación de todos los presupuestos necesarios para la aplicación de una pena.

- *Antijuridicidad*: se configura cuando determinados supuestos de hechos son contrarios al ordenamiento jurídico, sin que medie una causa de justificación que permita dicha acción en ciertas circunstancias y condiciones, expresamente desarrollados por la norma.

- *Culpabilidad*: se la considera como un juicio de reproche realizado con el fin de determinar si un suceso concreto, penalmente contrario al ordenamiento jurídico, es atribuible a un sujeto específico.

Es inevitable tener especial consideración en estos elementos, y a los fines de este trabajo aún más en la tipicidad, la cual se podría considerar que llego de forma tardía en cuanto a los fenómenos que aquí son objeto de estudio, aunque esto no lo hace menos importante, ya que en su defecto no se podría adentrarse en las vías judiciales atendiendo a los distintos principios que regulan el derecho penal, como lo son:

a) el *principio de legalidad:* el cual consagra a la ley penal previa como única fuente del derecho penal (nullum crimen, nulla poena sine lege[2]), es decir que es necesaria una tipificación anterior al hecho para no extender o sobrepasar los límites del numerus clausus del ordenamiento jurídico e incurrir en analogías perjudiciales al imputado, lo cual está prohibido en el derecho penal argentino, atento al art. 18 de la Constitución Nacional[3].

b) *principio de reserva:* les confiere a los individuos una zona inmune a todo tipo de sanciones, compuesta por todas aquellas conductas o acciones que no estén conformados y penados por una ley previa al momento en el que suceden. (Lascano, 2005) Este principio es configurado por la Constitución Nacional en el art. 19, 2do. Párrafo en el

[2] Aforismo en latín que expresa "Ningún delito, ninguna pena sin ley".
[3] Art. 18 de la CN: "Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso..."

cual se lee "Ningún habitante de la Nación será obligado a hacer lo que la ley no manda, ni privado de lo que ella no prohíbe".

Dicho esto, podemos dilucidar que es importante la enumeración taxativa de las acciones prohibidas por la ley para poder ser perseguidas penalmente, y es a esto a lo que se apuntaba ut supra.

Un importante antecedente[4] en la República Argentina, y que llama mucho la atención por lo antes desarrollado, fue el de la querella realizada contra el periodista Jorge Lanata, realizada por el Sr. Edgardo H. Martolio, acusándolo del delito de violación y publicidad de correspondencia, fundándose en los artículos 153 y 155 del Código Penal, e interpuesto ante el Juzgado Nacional Correccional Nº 6 de la Capital Federal. En este caso, el Sr. Lanata plantea un incidente de excepción de falta de acción por hecho atípico, el cual es rechazado por el juzgado. El acusado decide apelar la decisión, argumentando la atipicidad de los hechos que se le imputaban debido a que no se encontraban expresamente desarrollados en el ordenamiento jurídico hasta ese momento. La sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital federal, decide reafirmar la decisión del tribunal inferior. Ante este pronunciamiento, el querellado interpone un recurso de casación que es rechazado, por lo que luego se presenta un recurso de queja, el cual es desestimado, y en última instancia, la Cámara Nacional de Casación Penal resuelve: "...el tan difundido e-mail de nuestros días, es un medio idóneo certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos completos, etc....".

De esta manera, se ve como la interpretación judicial de las normas hace "expandir", si se quiere, los conceptos que hasta ese entonces ostentaban los artículos 153 y 155 del Código Penal que hacían referencia al apoderamiento y publicidad de correspondencia, incorporando a ella los "e-mails"; cuya palabra proviene de la abreviatura en inglés de "electronic mail", que en español su traducción sería "correo electrónico" y que se podría definirlos como una forma de transmisión de mensajes que se realiza entre dos computadoras que se encuentren conectadas a redes informáticas. Este medio de comunicación claramente no estaba contemplado en los artículos antes mencionados,

[4] Fallo: Martolio, Edgardo Héctor c/ Lanata, Jorge Ernesto s/ violación de correspondencia y publicidad. Juzg. Nac. Correccional N° 6 de la Cap. Federal. Año 1999.

porque su existencia fue posterior a la última modificación que hubiere "sufrido" el Código Penal hasta ese entonces, pero los jueces entendieron que se los podría considerar equivalentes a la recepción de la forma de correspondencia tradicional amparada por la legislación penal positiva.

Es realmente un caso que podría ser objeto de cuestionamientos, si justamente se plantea la atipicidad de los hechos hasta ese entonces, y la forma en que establece la equivalencia el juez de los medios de comunicación por e-mails y la correspondencia tradicional.

1.1.1 Características

Los delitos informáticos son perpetrados mayoritariamente por personas con cierto nivel de conocimiento en la materia, con status social y económico en términos generales altos; también los autores mantienen distancia o realizan estos actos sin contacto aparente con las víctimas, lo que genera una dificultad para ser concebido legal y socialmente como delincuente. Por eso mismo, es que se los considera "delitos de cuello blanco", cuya terminología fue utilizada por primera vez por el sociólogo norteamericano Edwin H. Sutherland en el año 1939.

Este tipo de delitos son cometidos en el mundo del "ciberespacio" lo que brinda una facilidad innegable a los individuos que los realicen, en cuanto al tiempo que les tomaría realizarlos teniendo en cuenta la inmediatez de la respuesta informática que otorgan las redes interconectadas, como así también con el aspecto físico que les permite controlar la situación prácticamente desde cualquier parte del mundo, sin encontrarse en el lugar donde se concreta el efecto de la conducta realizada.

Muchas veces es utilizada cierta posición ventajosa o algún tipo de situación que facilita la comisión de estos delitos, como podría ser la ejecución de una función dentro de organismos de sistemas relacionados a la tecnología o la economía, aunque otras tantas simplemente son realizados contra usuarios sin el conocimiento necesario para identificar las amenazas del mundo informático, ni sus propias vulnerabilidades.

Es importante mencionar el gran impacto económico que éste tipos de delitos provocan. Según una publicación de septiembre de 2018 del diario "La Nación"[5], los fraudes con tarjetas de crédito y débito conllevan una perdida diaria de ochocientos mil dólares (US$ 800.000) y se estima que para el año 2021, el costo de este tipo de delito global excederá los treinta y dos mil millones de dólares (US$32.000.000.000).

Por su parte, el diario "Clarín" en una publicación[6] a mediados del mismo año, afirma que el treinta y un porciento (31%) de las empresas que fueron el blanco de fraudes empresariales, sufrieron delitos informáticos.

Otra característica importante, y particularmente para el derecho, es la dificultad de perseguir estas conductas por la eliminación de pruebas y rastros, y las complicaciones a la hora de determinar el autor de estos delitos. Primeramente debido a lo que tiene como objeto el presente trabajo, la jurisdicción y competencia. Muchas veces los autores de estos delitos se encuentran fuera de la órbita de jurisdicción de los juzgados como así también de los fiscales que persiguen su condena; aun cuando la víctima y el victimario residen en el mismo lugar, es dificultosa la tarea de procesar a este último, por lo que es fácil imaginar lo tedioso que resulta cuando se encuentran en lugares diferentes. En el décimo primer Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2005)[7] se ha expresado que:

> La investigación y el enjuiciamiento efectivos de los delitos relacionados con las computadoras suelen requerir el rastreo de la actividad delictiva a través de una diversidad de proveedores de servicios de Internet o compañías con computadoras conectadas a la Internet. Para lograr el éxito, los investigadores deben seguir la pista de las comunicaciones hasta la fuente y las computadoras u otros dispositivos afectados, trabajando con proveedores de servicios intermedios en diferentes países. (p. 14).

[5] Listek, V. (2 de septiembre de 2018). Fraudes con tarjetas. En cajeros o en la web, un perjuicio anual de US$300 millones. La Nacion. Recuperado de https://www.lanacion.com.ar/seguridad/fraudes-tarjetas-en-cajeros-web-perjuicio-anual-nid2168221 el 25/05/2019.

[6] Quiroga, A. (10 de junio de 2018). Los delitos informáticos golpean al 31% de las empresas. Clarín. Recuperado de https://www.clarin.com/economia/delitos-informaticos-golpean-31-empresas_0_S1RZ3B_gX.html el 25/05/2019.

[7] 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Bangkok, 18 a 25 de abril de 2005. Recuperado de https://undocs.org/es/A/CONF.203/14 el 26/05/2019.

En el texto siguiente del mismo párrafo citado anteriormente, también se menciona que los mecanismos judiciales asistenciales tradicionalmente están dispuestos para obtener datos en circunstancias donde los involucrados son solo dos países, contrayendo mayores dificultades cuando estas actividades son realizadas con comunicaciones en una mayor cantidad de países, requiriendo de varios procesos de asistencia judicial para poder obtener los datos de los proveedores que ayuden a perseguir las pruebas; dilatando el tiempo y facilitando la desaparición de las mismas.

Siguiendo lo anteriormente mencionado podemos sintetizar que, la dificultad de perseguir a los "ciber-delincuentes" reside en la dificultad de reunir pruebas legales, debido a que, además de que estas personas mayoritariamente tienen el conocimiento técnico para eliminarlas, éstas no son tangibles ni tampoco tienen un tiempo de duración prolongado, ya que no es común el almacenamiento permanente de acciones en el mundo del internet, siendo más comúnmente la superposición de datos que eliminan al anterior; perjudicando además las dilaciones por la falta de asistencias judiciales internacionales que ostenten una aplicación global.

Estos problemas tienen como efecto colateral, la falta de denuncias de estas características, por lo que es dificultoso obtener estadísticas y números precisos acerca de este fenómeno, no obstante, no quedan dudas de la constante incrementación de estas conductas delictivas y la gran importancia de una solución globalizada efectiva.

1.1.2 Clasificación

La Organización de las Naciones Unidas, reconoce oficialmente cuatro tipos de delitos informáticos a saber, a los cuales definiremos con conceptos del Dr. Téllez Valdés, misma obra citada ut supra (2008):

1) Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de los datos de entrada: también conocido como sustracción de datos, no requiere conocimientos avanzados en informática para ser realizado, por lo que se lo considera como el ciberdelito más común.

- La manipulación de programas: consiste en transformar los programas existentes en el sistema o en introducir nuevos programas o tareas. Para realizar estas acciones si son necesarios ciertos conocimientos técnicos, los cuales también son utilizados para dificultar su descubrimiento y persecución.
- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada, donde ínfimas partes de las transacciones financieras se sustraen de una cuenta y se transfiere a otra.

2) Manipulación de los datos de entrada

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3) Daños o modificaciones de programas o datos computarizados

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- Virus: son claves programáticas que se introducen e infectan programas legítimos, con la tendencia a propagarse hacia otros.
- Gusanos: son fabricados de manera similar a los virus, pero no tienen el poder de regenerarse.
- Bomba lógica o cronológica: puede ser utilizado como herramienta para extorsionar a la víctima debido a que puede ser programada para que "explote" en un futuro, cuando el delincuente se haya retirado. Es difícil de detectar con anterioridad a la producción del daño.

4) Falsificaciones informáticas

- Acceso no autorizado a servicios y sistemas informáticos: puede realizarse desde la simple curiosidad hasta el sabotaje o espionaje informático.
- Piratas informáticos o hackers: comúnmente se realiza desde un sitio externo, los delincuentes aprovechan deficiencias en la seguridad o la vulneran para introducirse en el sistema como usuarios legítimos.
- Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Por otro lado, el 23 de noviembre de 2001, en la ciudad de Budapest, se estableció el convenio de cibercriminalidad[8], creado por el Consejo de Europa. En dicho instrumento se desarrollaron cuestiones básicas sobre la política penal de los países adheridos, con el objetivo de prevenir los delitos informáticos, promover la cooperación internacional y proponer mejoras legislativas al respecto.

La convención en el desarrollo de disposiciones de derecho material, realiza la siguiente clasificación de los delitos informáticos:

a) Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
   - Acceso ilícito.
   - Interceptación ilícita.
   - Atentados contra la integridad de los datos.
   - Atentados contra la integridad del sistema.
   - Abuso de equipos e instrumentos técnicos.

b) Infracciones informáticas.

[8] Convenio sobre Cibercriminalidad. Budapest, 23 de noviembre de 2001. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Convenio%20de%20Cibercriminalidad.Budapest.23.11.2001.pdf?idFile=641bfba0-bfde-4117-a260-1acb806880a6 el 29/05/2019.

- Falsedad informática.
- Estafa informática.

c) Infracciones relativas al contenido.

- Infracciones relativas a la pornografía infantil.

d) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

- Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Posteriormente, en el año 2008, con el fin de atacar los actos de racismo y xenofobia realizado a través de los sistemas informáticos, se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa", donde se estableció, entre otras cosas, las conductas a realizar en caso de:

-Difusión de material xenófobo o racista.

-Insultos o amenazas con motivación racista o xenófoba.

-Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Conclusión parcial

Teniendo en cuenta que a nivel mundial, los delitos informáticos no tienen un concepto universal que abarque a estas conductas, es lógico y entendible que nuestro sistema judicial aun no les haya dado un concepto univoco a estos fenómenos.

Por lo pronto, la única opción para todos aquellos que se adentren en el campo de estos delitos, deberán conformarse con optar por un concepto u otro, dado por los distintos autores de doctrinas diferentes, que van desde los que han considerado a estos delitos como únicos e independientes, hasta aquellos que los consideran una modalidad de los delitos tradicionales ya conocidos por el ordenamientos jurídico anterior a las nuevas incorporaciones en ésta materia.

Si bien el derecho tiene mucho trabajo de aquí en adelante para poder neutralizar esta, relativamente, nueva modalidad de delincuencia, ha sido un importante paso la enumeración taxativa de diferentes acciones punibles con la ley 26.388 en el año 2008, las cuales se explayarán en el próximo capítulo. Esto permite la investigación de las conductas lesivas y la persecución de los delincuentes que se hacen de este medio para lesionar los bienes jurídicos de las personas, lo cual anteriormente era un inconveniente al no haber estado tipificadas.

Estos delitos han acarreado un gran impacto económico y social, el cual aumenta con el pasar del tiempo. Si bien es difícil tener estadísticas claras acerca del número de delitos cometidos a través de las redes informáticas debido a la falta de denuncias y su difícil rastreo, se tiene por seguro que los índices escalan a grandes pasos por las constantes facilidades que el progreso tecnológico les ofrece a estos delincuentes, ya que prácticamente no se necesitan conocimientos técnicos avanzados para la realización de estos delitos.

Sumado a esto, las características existenciales de estos fenómenos también juegan a favor de la criminalidad, ya que es compleja la persecución de los autores que se esconden en el ciberespacio, teniendo la posibilidad de eliminar sus huellas, de estar a distancias descomunales del lugar del hecho y de ser "invisible" a la sociedad para ser tildados como delincuentes.

Por su lado los mecanismos asistenciales judiciales quedan obsoletos cuando las distintas acciones del delito y su resultado, tienen razón de ser en varios países, debido a que estos generalmente están hechos para la cooperación entre dos países para la obtención de información que ayude a las causas de investigación. Por ende sería importante el planteo de herramientas de cooperación internacional que tengan un carácter global, abarcando a la mayor cantidad de estados posibles, con el fin de perseguir este tipo de delitos y poder llegar a la sanción de los autores penalmente responsables.

CAPITULO II

PHISHING

Introducción

Este capítulo abordará como tema principal el "phishing", analizando tanto su concepto como las teorías acerca del origen de su nombre. Se desarrollará una breve historia de su nacimiento y su evolución a lo largo del tiempo.

Luego de conocer este fenómeno, su origen y componentes, este trabajo explayará los sujetos que son participes de esta relación, cuyas partes son: el sujeto pasivo y el sujeto activo.

Posteriormente, se tratarán los antecedentes legislativos, haciendo mención de la importante ley 26.388 del año 2008, cuya norma realiza la introducción de distintos delitos informáticos, que aunque no lo hayan hecho en un cuerpo normativo especifico que los regule, permitió la incorporación de conductas lesivas que no podían ser perseguidas por la justicia, al no estar revestidas de la tipificación requerida por ésta.

Lo antes dicho, dejará divisar que éste fenómeno se enmarcaría en el artículo 173 inciso 16 del Código Penal bajo una figura típica de estafa específica, regulándose mediante las medidas establecidas en el artículo 172 del mismo código, el cual trata la estafa tradicional, existente de forma anterior a la introducción de los delitos informáticos al cuerpo normativo que se ha hecho mención.

Para culminar con este capítulo, se intentará determinar el bien jurídico protegido de estos delitos, donde la mayoría de la doctrina entiende que ante las estafas informáticas, lo es el patrimonio como un todo, es decir, de forma holística. Sin embargo, hay expertos en el tema que afirman, debido a la pluriofensividad de este tipo de delitos, que también hay otros bienes jurídicos en juego que son potenciales víctimas de riesgo o lesión, por parte de los ciberdelincuentes.

2.1 Concepto

Hay dos teorías acerca del origen de la palabra "Phishing", según Steven Myers (2006), la primera es una evolución de la palabra "fish", cuyo significado en inglés es "pesca", a la cual se le habría reemplazado la letra "f" por "ph" (que en dicho idioma, al ser leídas, suenan de igual forma), lo cual era una práctica habitual en la jerga de los piratas informáticos.

Este término intentaría hacer alusión a la modalidad utilizada que pretende arrojar un "anzuelo" para que sea "mordido", metafóricamente hablando, por los individuos elegidos como objetivos.

La segunda teoría considera que dicha expresión proviene de la contracción de las palabras "password harversting fishing", lo cual significa "pesca y recolección de contraseña".

El Phishing es una forma de ingeniería social mediante la cual el atacante, conocido como "phisher", intenta obtener de manera fraudulenta los datos personales de identidad, de las cuentas bancarias y/o los de la tarjeta de crédito de las víctimas. (LLinares, 2012).

Esta técnica de fraude es realizada enviando correos electrónicos imitando el formato y contenido de páginas confiables, copiando todas sus características, haciéndolas prácticamente idénticas y procurando engañar la víctima para que efectivamente crea estar en una de ellas. De esta forma, por ejemplo imitando un mail enviado por una entidad bancaria, y utilizando artimañas, se le solicita a la persona que ingrese a una URL[9], la cual lo dirigirá a una página web pirata controlada por el "phisher", donde se le solicitará a la víctima que introduzca información confidencial en ella, por ejemplo completando un formulario con los datos de su tarjeta de crédito, para luego utilizarlos fraudulentamente.

Este tipo de ciberdelitos datan de los años noventa, se originaron a partir de la defraudación al sistema de American Online (AOL) creando cuentas falsas e introduciendo números de tarjetas de crédito que no correspondían a tarjetas reales. Si bien los datos de identidad y de las tarjetas de crédito ingresadas eran falsos, pasarían los protocolos de

[9] URL: son las siglas en inglés de Uniform Resource Locator, que en español significa Localizador Uniforme de Recursos.

seguridad de AOL, tomándolos el sistema como válidos. A partir de aquí, los hackers podrían utilizar los recursos del sistema sin riesgos y la cuenta permanecería activa hasta que AOL intentara facturar sobre la tarjeta otorgada.

Si bien hasta aquí lo realizado por los hackers no se consideraría "Phishing", las determinaciones de seguridad posteriores llevarían a estos a desarrollarlo. AOL mejoró la seguridad del sistema verificando de forma inmediata la validez de los números de tarjeta y la identidad de facturación ingresados. Como respuesta a esto, los ciberdelincuentes optaron por dejar de crear cuentas falsas y enfocarse en robar cuentas legítimas. La forma en que lo realizarían era por medio de mails o a través de la mensajería instantánea de AOL, haciéndose pasar por empleados de la compañía y solicitándoles a los usuarios su contraseña o información sobre sus tarjetas de crédito, para lo cual inventaban una historia que parecería creíble para que las victimas proporcionaren los datos solicitados. (Steven Myers, 2006)

A partir de aquí, el Phishing comenzaría a evolucionar dejando de atacar solamente a los servicios y clientes de AOL, para comenzar a hacerlo con distintas entidades financieras y de comercio electrónico, como así también a sus usuarios.

Según Fernando LLinares (2012), actualmente un ataque tradicional tiene tres componentes esenciales:

- El mensaje: los objetivos de este fraude reciben un reclamo vía correo electrónico, si bien no es sofisticado técnicamente, aprovecha las vulnerabilidades de las víctimas, quienes ingresarían a una URL donde ingresará la información perseguida por el hacker o instalará involuntariamente un malware[10] en su sistema.
- La interacción: una vez que la víctima recibe el mensaje, se intenta que ingrese a la web pirata creada de forma idéntica a la legitima de una entidad confiable, que ingrese la información anhelada por el hacker o que instale el malware.
- La utilización efectiva de la información robada: si bien algunas veces los victimarios utilizan personalmente los datos obtenidos,

[10] Malware: hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Recuperado de: https://www.avast.com/es-es/c-malware el 20/06/2019.

suplantando la identidad de la víctima, en la mayoría de los casos los datos son vendidos a terceros, quienes serán los que explotarán la información robada.

El Pharming, por su parte, es una nueva modalidad de fraude online que consiste en alterar o reemplazar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa. Su nombre proviene de la combinación de "phishing" y "farm" (granja, en inglés). Es una forma de phishing más sofisticada, donde un usuario ingresa una dirección web en su navegador, la cual debe ser transformada en una dirección IP numérica por el DNS, el cual, al ser hackeado, realiza esta acción redirigiéndolo a un sitio web falso. Una vez allí, se desarrollara el robo de información de la misma manera que el phishing tradicional desarrollado ut supra.

Una característica de esta modalidad, es que no se realiza en un determinado momento, sino que se modifica el DNS de los ordenadores, esperando a que el usuario haga uso de él al ingresar a sitios bancarios, para luego robar la información ingresada por estos.

2.2 Sujetos

Dentro de la acción delictiva denominada phishing, podemos encontrar dos sujetos identificables con facilidad como las partes necesarias para que concurra este tipo delictivo. Por una parte el sujeto activo, quien realiza la conducta delictiva y por otra, el sujeto pasivo, quien es el titular del bien jurídico lesionado por el primero. Ambas partes de la relación serán, a continuación, desarrolladas con sus respectivas características.

2.2.1 Sujeto activo

Si bien los sujetos que llevan a cabo este tipo de defraudaciones tienen un avanzado conocimiento informático, como así también sobre los medios utilizados para realizarlas, no es necesaria una cualificación especial por parte de éstos. Es decir que, la descripción típica desarrollada por el ordenamiento jurídico, no exige calidades específicas para ser el autor, sino que cualquier tipo de persona puede hacerlo. La importancia radica en que dicho sujeto altere el normal funcionamiento de un sistema informático o la

transmisión de datos, a través de una técnica de manipulación informática. (P. Lucero y A. Kohen. 2011)

El atacante en esta modalidad, como ya se ha expresado anteriormente en este trabajo, se lo denomina "phisher".

2.2.2 Sujeto pasivo

Como se ha anticipado, el sujeto pasivo de la relación es el titular del bien jurídico protegido. En su propio blog[11], Marcelo A. Riquert (2014) opina que es "aquel a quien patrimonialmente se perjudica mediante la manipulación del sistema o transmisión de datos, pudiéndose en muchos casos tratarse no sólo de personas físicas sino de existencia ideal, como compañías financieras, bancarias, bursátiles, aseguradoras, etc."

Es decir que también puede ser sujeto pasivo cualquier persona, física o jurídica, requiriéndose simplemente que sea el propietario de los bienes jurídicos que pueden ser lesionados. Dicho de otra manera, podrá sujeto pasivo todo aquel que pueda ser el damnificado por la disposición patrimonial llevada a cabo en esta modalidad de defraudaciones electrónicas.

2.3 Antecedentes legislativos

Finalizando el año 2001, la Secretaria de Comunicaciones trabajó en un proyecto de ley, el cual estaba compuesto por cinco artículos autónomos que proponían penalizar el daño informático, el acceso ilegitimo y el fraude informático.

Más adelante, debido a un inconveniente suscitado por el reemplazamiento de la página del Poder Judicial por un archivo con escritos de carácter político, y a que un juez federal debió declarar atípica dicha conducta; la Corte Suprema de Justicia le requirió al Ministerio de Justicia que confeccionara un proyecto de ley para suplir el vacío, el cual se realizó en conjunto con el Ministerio Publico y fue elevado al Presidente de la Nación en mayo de 2002. Dicho proyecto contenía una considerable reforma del Código Penal sobre delitos informáticos, cuyo contenido no se desarrollará en razón de brevedad.

[11] http://riquertdelincuenciainformatica.blogspot.com/2014/11/estafa-o-fraude-informatico.html Recuperado el 15/08/2019.

Sin embargo, el anteproyecto que sirvió de inspiración para la reforma del código Penal fue realizado en el año 2005 por los Ministerios de Justicia y Relaciones Exteriores. Si bien no obtuvo estado parlamentario, dejo en evidencia que los ministerios mencionados expresaban oficialmente la necesidad de penalizar conductas informáticas. (Palazzi, 2016)

En el año 2006, más precisamente en el mes de mayo, el Anteproyecto de Ley de Reforma y Actualización integral del Código Penal, fue presentado en consulta pública. A través del Ministerio de Justicia y Derechos Humanos de la Nación, se fundó la "Comisión para la Elaboración del Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal.

Dicho instrumento de reforma contenía diversas alteraciones en el campo tecnológico, que si bien no se desarrollarán, se mencionará por la incumbencia con el objeto de este trabajo, que en el capítulo IV que hacía referencia a estafas y otras defraudaciones, no se regulaba a la estafa informática, contrariamente a lo que había planteado el anteproyecto de la comisión interministerial.

En ese entonces, a mediados del corriente año, se producen altercados por la violación de correos electrónicos de jueces y periodistas, que tomaba una creciente importancia debido a una denuncia proveniente de un importante diario de la capital, denotando la indiscutible reiteración de intrusismos en los teléfonos y correos electrónicos de periodistas, como así también la falta de regulación por parte del cuerpo legislativo nacional, que dejaba a estas conductas sin sanción penal por no incurrir en delito alguno.

Esto desembocó en un debate de un proyecto de modificación del Código Penal, por parte de las comisiones de Legislación Penal, Comunicaciones y Libertad de Expresión de la Cámara baja. A partir de lo dicho, se desencadenó otra variedad de proyectos relacionados a los correos electrónicos que fueron presentados en el congreso.

Para fines de junio de 2006, el congreso contaba con dieciséis proyectos relacionados a los correos electrónicos y los delitos informáticos. Esto hizo que este órgano tomara esta oportunidad denotada por el interés en legislar, para reformar no solo haciendo referencia a los correos electrónicos sino también a otros ciberdelitos.

A fines del año 2006, la cámara de diputados aprobó el proyecto de ley, el cual contenía entre otros delitos tradicionales, a la estafa informática.

Al correr el año siguiente, 2007, el Senado estudió el proyecto y luego de algunas reformas que mejoraron la técnica legislativa y otras consideraciones atendiendo a las opiniones de diferentes expertos consultados en las reuniones que abordaron el tema, el 28 de noviembre fue aprobado.

Por último, la Cámara de Diputados aceptó las reformas propuestas por el Senado y dio por aprobado el texto final, dando origen a la promulgación de la Ley 26.388 el 24 de junio de 2008 y publicándose en el Boletín Oficial al día siguiente.

Por ende, los delitos informáticos recién en el año 2008 fueron receptados por el código penal argentino, a partir de dicha norma, la cual realiza incorporaciones, modificaciones, y sustituciones de diferentes figuras simples que se regulaban hasta ese momento. Las partes incorporadas por esta ley que se podrían considerar atinentes a los delitos a los que apunta este trabajo, son:

1) La incorporación a los últimos párrafos del artículo 77 del Código Penal, expandiendo el término "documento" a toda representación de actos o hechos, sin importar el soporte utilizado. Comprender los términos de "firma" y "suscripción" como firma digital, la creación de una o realizarla digitalmente. Utilizar los términos "instrumento privado" y "certificado" equivalentes al documento firmado de manera digital.

2) Sustitución del epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por "Violación de secretos y de la privacidad".

3) Sustitución del artículo 153 del Código Penal, estableciendo prisión de quince (15) días a seis (6) meses al que abriere, accediere, se apoderare, suprimiere o desviare indebidamente una correspondencia o comunicación electrónica; como así también al autor de la captación o intercepción de ellas provenientes de sistemas privados o de acceso restringido.
En los casos en que el autor, además, comunique o publique el contenido, la pena será de un (1) mes a un (1) año de prisión.
En los casos de que alguno de estos delitos fuere cometido por un funcionario público, se

establece que recibirá también la inhabilitación especial por el doble de tiempo de la condena.

4) Incorporación del artículo 153 bis, en el cual se estipula la pena de quince (15) días a seis (6) meses de prisión, al que a sabiendas y sin autorización o excediéndose de ésta, accediere a un sistema o dato informático de acceso restringido; y en cuyo caso estos últimos pertenecieran a un organismo público estatal, o a un proveedor de servicios públicos o financieros, la pena impuesta es de un (1) mes a un (1) año de prisión.

5) En la sustitución del artículo 157 bis se establece que será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: "A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".

6) La interesante y más importante incorporación, respecto a lo que a este trabajo le interesa, del inciso 16 al artículo 173[12] del Código Penal, el cual reza: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

7) Incorporación de un 2do párrafo al artículo 183 del Código Penal, el cual le otorga una pena de quince (15) días a un (1) año de prisión al que "alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Bien jurídico protegido

Sin perder la atención en lo desarrollado anteriormente, se puede dilucidar que la defraudación informática, en nuestro ordenamiento jurídico, se encuentra incorporado por el inciso 16 del art. 173 que enumera los casos especiales dentro de la figura de la estafa, la cual se encuentra desarrollada de forma típica y genérica en el art. 172 del Código Penal. Esto quiere decir, en otras palabras, que la estafa informática es una modalidad específica,

[12] El artículo 173 del Código Penal establece cada uno de los acontecimientos que serán considerados como casos especiales de defraudación, estableciendo a ellos la pena del art. 172 del mismo código (prisión de un mes a seis años)

de la figura tradicional plasmada en el Código Penal anteriormente a la reforma del año 2008, la cual tiene por bien jurídico protegido, en términos generales, a la propiedad.

Ahora bien, la discusión actual se centra en determinar si el bien jurídico protegido es la propiedad en sí, o si lo es el patrimonio, especialmente.

Por su parte P. Lucero y A. Kohen (2011) expresan:

> Nos inclinamos por pensar que el bien jurídico protegido es más bien el patrimonio, ya que con la conducta lesiva se afecta holísticamente el patrimonio mismo del damnificado y no un componente de la propiedad de dicho sujeto pasivo, como podría ser el caso de los delitos de hurto o robo.
>
> Es que resulta técnicamente más adecuado hablar de delitos contra el patrimonio, pues no sólo se incluyen acciones que lesionan o ponen en peligro la propiedad, sino también aquellas que afectan a otros valores patrimoniales como la posesión, el derecho de crédito, e incluso las expectativas. (p. 75)

Así como los autores anteriormente citados, la parte mayoritaria de la doctrina sostiene que el bien jurídico protegido ante las estafas informáticas es el patrimonio. Sin embargo, teniendo en cuenta la característica de pluriofensividad que ostentan los delitos informáticos, que permite la lesión de distintos bienes jurídicos a la vez, podría afirmarse que el phishing afecta también la privacidad –al acceder a la información de carácter confidencial e identificatoria- , el honor –en los casos que se contraigan obligaciones a nombre del afectado- y por otra parte, también se podría considerar la fe pública como otro bien jurídico lesionado, al tener presente la necesidad de la confianza de los usuarios para llevar a cabo éste ilícito.

Conclusión parcial

Estos delitos tienen una existencia considerable en el tiempo, sin embargo el derecho ha incorporado recién hace poco más de diez años instrumentos normativos para

intentar traer soluciones a las víctimas, a los encargados de investigar y perseguir delitos, y a los órganos encargados de impartir justicia.

No obstante, aún está vívido el sentimiento de insuficiencia que provocan las herramientas con que cuenta la justicia para combatir la delincuencia informática.

La constante evolución que demuestran estos fenómenos hace considerar preocupante la incapacidad de la ley para amoldarse al dinamismo de la tecnología utilizada para delinquir, debido a los potenciales modos de phishing que puedan seguir surgiendo con el tiempo ya que, aun con los ya existentes, se producen considerables inconvenientes para lograr la penalización de los autores.

Como se ha visto, estos delincuentes llamados "phishers" no necesitan una cualificación especial, y si bien históricamente se ha considerado que ostentan un avanzado conocimiento informático, la evolución mencionada hace que los distintos procedimientos utilizados para llevar a cabo estas conductas lesivas, sean cada vez más simples y automatizados, provocando que una mayor cantidad de personas inexpertas en el tema puedan llevar a cabo estos delitos, o al menos intentarlo.

En consecuencia, se han incrementado con el pasar del tiempo la cantidad de defraudaciones por medio de esta modalidad, lo que provoca un mayor impacto a los bienes jurídicos protegidos de las personas físicas y jurídicas, ya que como se ha explicado, las victimas pueden ser las personas físicas, las empresas o las instituciones.

La Ley 26.388 de Delitos Informáticos trajo consigo la solución a la problemática que presentaba la imposibilidad de engañar o estafar a una maquina u ordenador, lo que provocaba que los ahora considerados fraudes informáticos, recayeran en delitos de hurto por ejemplo.

Sin embargo, la falta de una regulación procesal penal aun hace que estos delitos sean interpretados sin la certeza suficiente, y provoca que aun exista un vacío legal respecto a la investigación y a los procedimientos de recolección de material probatorio.

CAPITULO III

COMPETENCIA

Introducción

El presente capitulo profundizará la temática de mayor relevancia para este trabajo, la competencia. Para esto primeramente será importante aclarar el concepto de jurisdicción, debido a que la competencia es una medida en la que se puede ejercitar esta última.

Posteriormente, se identificará la competencia ordinaria y la federal, que según la doctrina que se citará, la primera de ellas es la elegida para conocer en los casos de delitos informáticos, en líneas generales.

Luego, el desarrollo de éste capítulo se adentrará en los inconvenientes suscitados en la práctica ante la aplicación de las herramientas que el derecho le ha otorgado a la justicia, las cuales fueron insuficientes para la determinación de la competencia de una forma precisa. Por lo que, a continuación de ello, se desarrollaran las teorías utilizadas para determinar el lugar del hecho, cuando la acción realizada y el resultado de ella surgen en distintos lugares geográficos.

Para finalizar, se hará alusión a distintos casos jurisprudenciales que pusieron de manifiesto las interpretaciones de la casuística ante estos fenómenos, que ante la falta de una regulación procesal penal respecto a estos fenómenos tecnológicos, ha sido utilizada como fuente para solucionar los conflictos de competencia negativa entre los diferentes órganos judiciales.

3.1 Competencia judicial

Para poder conceptualizar a la competencia, primero hay que tener conocimiento de lo que es la jurisdicción.

La jurisdicción es el poder que ostenta el estado de juzgar o de ejercer la función judicial, cuya facultad le corresponde al poder judicial y a sus miembros. En cambio, la competencia es la facultad para ejercer dicho poder, en un conjunto de casos concretos, que la ley le otorga a un tribunal determinado.

En síntesis, la competencia es la medida en que se puede ejercitar la jurisdicción. (Torres Neuquén, 2008).

3.1.1 Competencia Ordinaria y Federal

El estado argentino, al tener un sistema de gobierno federal establecido en el art. 1 de su Constitución Nacional[13], posee de justicia federal u ordinaria, donde esta última también se ramifica en provincial o local. Por ende, en los nacimientos de conflictos que activen los mecanismos judiciales, es importante determinar cuál de ellas debe actuar.

Para esto, es de gran relevancia lo expresado por el art. 116 de la Constitución Nacional:

> Corresponde a la Corte Suprema y a los tribunales inferiores de la Nación, el conocimiento y decisión de todas las causas que versen sobre puntos regidos por la Constitución, y por las leyes de la Nación, con la reserva hecha en el inciso 12 del artículo 75: y por los tratados con las naciones extranjeras: de las causas concernientes a embajadores, ministros públicos y cónsules extranjeros: de las causas de almirantazgo y jurisdicción marítima: de los asuntos en que la Nación sea parte: de las causas que se susciten entre dos o más provincias; entre una provincia y los vecinos de otra; entre los vecinos de diferentes provincias; y entre una provincia o sus vecinos, contra un Estado o ciudadano extranjero.

[13] Artículo 1º de la Constitución Nacional: La Nación Argentina adopta para su gobierno la forma representativa republicana federal, según la establece la presente Constitución.

Dicho artículo, deja asentada la competencia de la justicia federal excepcionalmente a los asuntos mencionados en él, correspondiéndole a la justicia ordinaria, el resto de los casos.

3.1.2 Competencia en los Delitos Informáticos

De acuerdo con P. G. Lucero y A. A. Kohen (2011), las figuras típicas establecidas por la ley de delitos informáticos, por lo general, están dadas con la intervención de la justicia ordinaria local. Dichos autores sostienen que la codificación, la jurisprudencia y la doctrina asignan coincidentemente la competencia relacionada al sitio donde fue realizado el hecho, satisfaciendo de este modo al principio legal general del artículo 18 de la constitución nacional, que consagra la noción del "juez natural".

Esto quiere decir que, las causas suscitadas dentro del territorio que la ley les confiere a los jueces para ejercer su jurisdicción, serán el lugar donde actuará la justicia. El fin perseguido con ésta lógica es favorecer la defensa en juicio, como así también al principio de economía procesal a través de la más rápida y simple investigación.

Ahora bien, las características que ya fueron mencionadas anteriormente en este trabajo, como lo son la transnacionalidad y la atemporalidad de los delitos informáticos, hace que las regulaciones establecidas no puedan amoldarse a ellos. El nuevo "territorio" donde los delincuentes llevan a cabo sus acciones, como ya se ha dicho, es el ciberespacio, que rompe con los espacios físicos tradicionales, traspasando incluso barreras fronterizas entre los estados de todo el mundo.

Como consecuencia de esto, se originan importantes inconvenientes para el derecho a la hora de determinar el lugar de comisión del hecho, la ley que debe aplicarse, y la competencia del órgano que conocerá el caso.

El derecho procesal penal requiere de forma imperante, a partir de los principios constitucionales receptados por él, que todo procedimiento señale el sitio donde es cometido el hecho ilícito para que pueda otorgarse la aplicación de la ley penal en un territorio especifico y ser aplicada por los órganos establecidos para conocer en la causa, para luego juzgar a los imputados. Esto le da origen al principio de territorialidad, el cual se entabla por referencias geográficas que determinan el lugar de la comisión del hecho dentro

de determinados límites fronterizos, ya sea en jurisdicciones internacionales o de un mismo estado. (Ruiz. 2018)

Esto último es utilizado como fundamento para la competencia territorial, cuya potestad jurisdiccional es ejercida por el juez en un determinado territorio, como manifestación de la soberanía del estado reconocida por la comunidad internacional. Dicha competencia se basa en lo expresado en el Código de Procedimiento Penal de la Nación, en su artículo 37, el cual reza:

> Será competente el tribunal de la circunscripción judicial donde se ha cometido el delito. En caso de delito continuado o permanente, lo será el de la circunscripción judicial en que cesó la continuación o la permanencia. En caso de tentativa, lo será el de la circunscripción judicial donde se cumplió el último acto de ejecución.

Como regla subsidiaria, el artículo 38 del mismo código, expresa: "Si se ignora o duda en qué circunscripción se cometió el delito, será competente el tribunal que prevenga en la causa."

Lo anteriormente dicho, no presentaba mayores dificultades en los delitos cometidos a distancia, debido a la cooperación internacional en el ámbito judicial como solución a la ejecución y cumplimiento del juzgamiento en una jurisdicción especifica. Sin embargo, el potencial traspaso de fronteras que ostentan los delitos informáticos, hacen que los parámetros para la ubicación del sitio donde fuera cometida la conducta lesiva y la producción del resultado de ésta, sean imprecisos. En casos prácticos, un delito podría atravesar los límites fronterizos de distintos países, pudiendo iniciarse en uno con leyes diferentes a la de otro u otros, donde se produciría el resultado de la acción, pudiendo también sus efectos expandirse a otros lugares geográficos, provocando riesgos y/o lesiones a victimas indeterminadas. (Ruiz. 2018)

Esto quiere decir, además, que los distintos ordenamiento jurídicos de los diferentes estados podrían ser incompatibles, donde en unos estén tipificados ciertos supuestos punibles que en otros no lo estén, creando posibles ámbitos de impunidad, vacíos legales, y facilidades de los autores de los delitos para evadir a la justicia.

3.2 Teorías sobre el lugar del hecho

Hay tres miradas a través de las cuales se intenta solucionar los inconvenientes para establecer la competencia de los juzgados en los casos donde la acción y el resultado se lleven a cabo en distintos lugares:

1) Teoría de la acción o de actividad

Esta teoría entiende que el lugar donde fue cometido el acto delictivo es en donde toda la acción o parte de ella fue realizada. Es decir que se tendrá en cuenta la ley del estado donde el autor despliega o produce la acción, sin importar donde surta efecto el resultado del delito.

Este pensamiento encuentra fundamento en que, si fuera de otro modo, no se podría castigar los delitos que no tienen un resultado, como en los casos de tentativa por ejemplo, cuya situación podría darse en el delito objeto de estudio en este trabajo, de lo cual P. G. Lucero y A. A. Kohen expresan:

> ...como en todo delito de resultado, la tentativa es admisible.
> En ese sentido, la tentativa existirá a partir de que el autor despliegue su técnica de manipulación informática y durante todo el proceso que implicará el desenlace final del perjuicio patrimonial, dentro del cual podemos incorporar a la disposición patrimonial.
> Es decir que habrá tentativa si no se ha producido el perjuicio patrimonial, aunque se hayan realizado diversas acciones con el fin de defraudar. (p. 79)

Por otro lado, es importante mencionar que en los casos de phishing y pharming, es difícil determinar el lugar donde se pone en marcha la conducta, para lo que se necesitan personas expertas en la materia que lleven a cabo la realización de las investigaciones pertinentes. Sin embargo, aun recolectando información sobre el tráfico de datos y determinando la ubicación de la dirección IP a través de la cual se realizan las acciones, no resultan suficientes para convertirse en pruebas inmediatas, ni otorgan la certeza suficiente de donde fueron cometidas.

Obviamente el proceso investigativo lleva su tiempo, y sumándole la dificultad que crea el ciberespacio para la detección de los autores, como así también de pruebas útiles, en muchos casos esto provocará que sea posible ver con anterioridad el lugar donde surten los efectos de la conducta ilícita realizada y más tarde, o nunca, desde donde provienen. (Ruiz, 2018)

2) Teoría del resultado

Dicha teoría, por su parte, sostiene que el lugar de comisión del delito es donde se produce el resultado, esto quiere decir, en otras palabras, que se tendrá como lugar del ilícito donde se produzca el daño o la lesión. Debido a esto es que el estado que sufre la perturbación del orden es el facultado para ejercer su jurisdicción, es decir que es el que tendrá la potestad de juzgar y sancionar en el proceso.

Como consecuencia de lo anteriormente dicho, Maximiliano Ruiz (2018) expresa que:

> ...si los resultados lesivos de una conducta se perciben en varios países, en forma simultánea o en periodos temporales distintos y que alcanzan a una pluralidad de víctimas, provocará una atomización de sumarios dando lugar a tramitaciones paralelas con una superposición de actividades probatorios pudiendo, eventualmente, dar lugar a soluciones procesales divergentes y a pronunciamientos contradictorios, generándose así un peligro de sometimiento a un doble (o múltiple) riesgo procesal (non bis in ídem).

Esto significaría que al aplicar esta teoría, se podrían generar inconvenientes jurisdiccionales al haber distintos países, donde surtieron efectos los resultados del delito, con la posibilidad fundada de solicitar para sí, la potestad de juzgar y sancionar estas conductas delictuales.

3) Teoría de la ubicuidad

Según ella, el delito debe reputarse cometido en el lugar donde se lleva a cabo toda o parte de la acción, como así también donde se produzcan los resultados con todos sus efectos. Significando que los hechos serán considerados cometidos en la totalidad de los sitios en los que se realizó la acción, desde su inicio hasta su fin. (Ruiz, 2018)

Esta perspectiva ayuda a la determinación de la competencia territorial en los casos que se han planteado anteriormente, donde las acciones delictivas son realizadas en el ciberespacio con las ventajas para los delincuentes, que ya se han desarrollado en este trabajo, aún más en las primeras etapas de investigación, donde se incrementan las dificultades en la búsqueda para descubrir instrumentos probatorios.

Esta doctrina es dominante en el derecho comparado, en el Código Penal Alemán por ejemplo, su artículo Nº 9 expresa:

> Un hecho es cometido en el lugar en el que el autor ha actuado o, en los casos de la omisión en que debería haber actuado o en el lugar en el que se ha producido el correspondiente resultado al tipo penal o en el lugar en donde según la percepción del autor ha debido producirse.
>
> La participación se comete no solo en el lugar en el que se comete el hecho sino también en aquel lugar en el que el participe ha ya actuado o en los casos de omisión debería haber actuado o, en el lugar en el que según la percepción del partícipe el hecho debería haberse producido. Si el participe ha actuado en el territorio nacional para un hecho en el exterior, entonces rige para el participe el derecho penal alemán también cuando el hecho no está amenazado con una pena conforme al derecho del lugar del hecho.

El Código Penal de Costa Rica también se inclina por la teoría de la ubicuidad, ya que en su artículo Nº 20 se puede leer:

> El hecho se considera cometido: a) En el lugar en que se desarrolló, en todo o en parte, la actividad delictuosa de autores o partícipes; y b) En el lugar en que se produjo o debió producirse el resultado...

También es la teoría por la cual opta el Código Penal de Italia en su artículo Nº 6, el cual expresa:

> Cualquier persona que cometa un delito en el territorio del Estado es castigada de acuerdo con la ley italiana.
>
> El delito se considera cometido en el territorio del Estado, cuando la acción u omisión que lo constituye, ha ocurrido allí en su totalidad o en parte, o donde ocurrió el evento que es consecuencia de la acción u omisión.

Por el mismo camino los siguen, por ejemplo, los Códigos Penales de Suiza y de Portugal en sus respectivos artículos Nº 7 de sus cuerpos normativos.

España, por su parte, también es partidaria de la teoría de la ubicuidad para los casos de los delitos a distancia, sin embargo considerando casos jurisprudenciales de delitos informáticos, se ha decidido por establecer un criterio diferente. La Sala Penal del Tribunal Supremo en autos con fecha de 03 de julio de 2015[14] declara en su parte pertinente, a lo que nos interesa, que:

> ...es verdad que esta Sala tiene declarado que el delito de estafa se entiende cometido en todos los lugares en los que se han desarrollado las acciones del sujeto activo (engaño) o del sujeto pasivo (disposición patrimonial) y en el que se ha producido el perjuicio patrimonial (teoría de la ubicuidad). Este punto de vista viene corroborado por el Pleno no jurisdiccional de esta Sala de fecha 3 de febrero de 2005, en el que se tomó el siguiente acuerdo: *"El delito se comete en todas las*

[14] Cuestión de competencia, resuelta el 03 de julio de 2015, Sala Segunda de lo Penal del Tribunal Supremo de España. Recuperado de: https://supremo.vlex.es/vid/577771866 en fecha 02/09/2019.

> *jurisdicciones en las que se haya realizado algún elemento del tipo, en consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa"...*
>
> ... En efecto, no obstante la teoría de la ubicuidad, (ver auto de 6.42011), ha proclamado que en estos supuestos de estafa informática no sirven para dirimir la competencia ni el " *criterio de la emisión de correos"* , que supone el inicio de la trama defraudatoria, pues nos puede conducir al extranjero o a la nube Informática ni los criterios de residencia de los titulares de cuentas corrientes o domicilios de las víctimas del delito, *puesto que el verdaderamente relevante es el de "lugar de actuación y residencia del intermediario o mula" pues es allí donde la investigación policial puede tener algún éxito, donde se han realizado elementos del delito, donde puede operarse sobre los ordenadores informáticos y donde la instrucción puede ser eficaz* . En definitiva, en los delitos informáticos, el criterio de la eficacia en la instrucción desplaza a la teoría de la ubicuidad.

Siguiendo el hilo de dicho razonamiento, en el mismo fallo citado, el Tribunal Supremo español declara:

> En definitiva, en los delitos informáticos, el criterio de la eficacia en la instrucción desplaza a la teoría de la ubicuidad. [...] Y por último decir que a la misma conclusión se llegaría si tuviéramos en cuenta el criterio de la mayor facilidad y conveniencia en la investigación, también utilizado por nuestra jurisprudencia, y mantenido en este tipo de delitos por el Convenio sobre el Cibercrimen, suscrito en Budapest el 23 de noviembre de 2001, ratificado por España el 27-9-2010, que determina que será competente el Estado " *que esté en mejores condiciones para ejercer la persecución del delito* " (artículo 22.5).

3.3 Perspectiva adoptada por Argentina

Como se puede dilucidar al conocer el primer artículo[15] del Código Penal Argentino, principalmente en el inciso 1, que declara que dicho cuerpo normativo se aplicará "por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción"; se ha optado por la teoría de la ubicuidad.

Esto quiere decir que se podrá tener en cuenta para determinar la competencia, el lugar donde se ha llevado a cabo la acción delictiva, en este caso la manipulación informática, como así también el lugar donde se produce el resultado, siendo éste, la disposición patrimonial.

Empero, como se ha reiterado varias veces, se generan inconvenientes a la hora de establecer la competencia en este tipo de delitos debido a la complejidad de la determinación del fórum delicti comissi, es decir, el lugar donde se ha cometido el delito.

Como posible solución a ésta problemática, el principio de ubicuidad establece que todos los sitios donde se hayan cometido elementos de la conducta delictiva, y donde se hayan producido los efectos de ésta, será considerada como jurisdicción en la que fue cometida el delito, permitiendo así a los jueces de dichas ubicaciones ostentar competencia territorial.

Ahora bien, en los delitos de defraudación informática se podría considerar a la disposición patrimonial, es decir el perjuicio económico, como el factor de mayor relevancia a la hora de establecer la competencia territorial, por lo que se preferirá la ubicación donde se hayan realizado las transacciones económicas en la cuenta bancaria del titular, sin su consentimiento. (Ruiz, 2018)

En concordancia con lo dispuesto, la jurisprudencia en un caso específico habría considerado oportuno declarar la competencia del juzgado ubicado en el lugar donde se

[15] Artículo 1 del Código Penal Argentino: Este Código se aplicará: 1) Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción. 2) Por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo. 3) Por el delito previsto en el artículo 258 bis cometido en el extranjero, por ciudadanos argentinos o personas jurídicas con domicilio en la República Argentina, ya sea aquel fijado en sus estatutos o el correspondiente a los establecimientos o sucursales que posea en el territorio argentino.

habían realizado los movimientos bancarios para la obtención patrimonial por parte del delincuente, declarando:

> El lugar de emisión de los correos por parte de la empresa contratante y el lugar de residencia del titular de la cuenta bancaria víctima del delito, son datos que resultan irrelevantes al efectos de la instrucción de la causa. Siendo datos trascendentes el lugar de actuación y de residencia del intermediario, al ser donde se reciben las transferencias y se extrae materialmente el dinero del circuito bancario para su envío a destinos en el extranjero; y también el lugar de emisión de la orden de transferencia, que no siempre se puede precisar. (Como fue citado por Ruiz, 2018)

No obstante, el Convenio de Cibercriminalidad de Budapest propone otra opción, en la cual Argentina ha basado resoluciones en ciertos casos de competencia negativa entre diferentes juzgados, además de establecer la posible solución en los casos donde las jurisdicciones que se contraponen son de distinta nacionalidad.

Dicho instrumento establece en su artículo 22 inciso 1, que las partes deben adoptar las medidas necesarias para atribuirse la competencia de las infracciones penales que han sido establecidas desde el articulo 2 al 11 del convenio, cabiendo destacar que el articulo 8 desarrolla de forma específica al fraude informático. No obstante, la parte de mayor relevancia a los fines de lo que se plantea, es lo plasmado por el inciso 5:

> En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir que jurisdicción es más adecuada para entablar la acción penal.

Para comprender de forma más acabada las decisiones judiciales siguiendo la lógica desarrollada ut supra, se destacarán a continuación algunos ejemplos jurisprudenciales en orden cronológico respecto al año en el que han sucedido las contiendas.

En el año 2010 se da un caso[16] de competencia negativa entre el Juzgado Nacional en lo Criminal de Instrucción Nº 12 y el Juzgado de Garantías Nº 5 de la ciudad de Mendoza, en cuya causa se investigaba una denuncia de delitos de estafa. El denunciante habría declarado que una persona cuya identidad desconocía, habría realizado diferentes compras de distintos productos a proveedores diferentes a través de internet, a quienes les enviaba comprobantes de pagos apócrifos, que obviamente nunca se habían realizado. De esta manera, aquellos proveedores que consideraban a estos tickets como válidos, enviaban la mercadería acordada a través de encomiendas a la ciudad de Mendoza, siendo de esta forma, engañados.

El juzgado nacional negó tener competencia, basando su argumentación en que la defraudación fue consumada con la recepción de la mercadería obtenida de manera fraudulenta por parte del delincuente; declinando de este modo la competencia a favor del Juzgado de Garantías con jurisdicción en Mendoza.

El juez provincial, argumentando que el desplazamiento patrimonial se realizó en la Capital Federal a partir del envió de una de las encomiendas, decidió rechazar la competencia atribuida.

Al regresar al magistrado de origen, éste reafirmó su decisión en cuanto al inconveniente tratado, por lo que se trabó la contienda.

Este caso se resolvió aplicando la teoría de la ubicuidad, teniendo en cuenta el lugar donde se desarrolla el ardid, como el lugar donde se produce la disposición patrimonial, para establecer la competencia territorial; la cual se estableció, particularmente en esta contienda, basándose en razones de economía procesal.

Hay que tener especial consideración que en este caso hubo una variedad de jurisdicciones donde se llevaron a cabo las disposiciones patrimoniales de diferentes víctimas, por lo que se optó por establecer la competencia en el lugar del ardid.

[16] Jurín Istueta, Aldo Nicolás. 26 de Octubre de 2010. Corte Suprema de Justicia de la Nación, Capital Federal, Ciudad Autónoma de Buenos Aires. Recuperado de http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-jurin-istueta-aldo-nicolas-fa10985852-2010-10-26/123456789-258-5890-1ots-eupmocsollaf el 10/09/2019.

Posteriormente, en el año 2015, se da otro caso[17] de competencia negativa entre el Juzgado Nacional en lo Criminal de Instrucción y el Juzgado de Garantías Nº 4 del departamento judicial de Bahía Blanca, de la provincia de Buenos Aires. Dicha causa se originó con la denuncia del damnificado, quien manifestó que a través de la plataforma de home banking del Banco Galicia se habría realizado una transferencia por un importante monto de dinero, a otra cuenta a nombre de Fernando Carlos M. en una sucursal de la misma entidad bancaria sita en la ciudad de Bahía Blanca.

El magistrado nacional entendió que la maniobra se consumó en territorio provincial, por lo que declinó su competencia.

El Juzgado local también rechazó la competencia atribuida, argumentando que la disposición patrimonial se habría realizado en la Ciudad Autónoma de Buenos Aires.

Vuelta al tribunal de origen, éste mantuvo su postura por lo que se trabó la contienda y se elevó a la corte.

El Procurador Fiscal de la Nación, basándose en razones de economía procesal y teniendo en cuenta los lugares donde se habrían realizado actos con relevancia típica, declaró:

> En esta inteligencia, más allá de que la cuenta bancaria de la que se dispusieron los fondos se encuentra en esta ciudad, donde además se habría accedido a internet para efectuar la transferencia, entiendo que corresponde declarar la competencia ·del magistrado local pues es el que se encuentra en mejores condiciones para continuar con la causa, en atención a que en su ámbito territorial se encuentra la entidad a la que se transfirió el capital (fojas 38) y se domicilia su titular (fojas 32), sumado a la circunstancia de que en la fecha en la que se efectuó la operación se registran en el extracto bancario numerosas entradas de dinero mediante el sistema de home banking.

Atendiendo a las palabras del procurador, transcurriendo el año 2016, la Corte Suprema de Justicia estableció la competencia en el Juzgado de Garantías Nº 4 del departamento judicial de Bahía Blanca.

[17] N.N. s/estafa damnificado E , Alejandro Raúl CCC 42073/20 1 5/IICS 1. Corte Suprema de justicia de la Nacion, 18 de octubre de 2016.

En el año mencionado, 2016, se desarrollaron los dos siguientes fallos. El primer fallo de competencia negativa al que se hará alusión es el originado entre los titulares del Juzgado Nacional en lo Criminal de Instrucción Nº 24 y del Juzgado de Garantías Nº 2 del departamento judicial de Lomas de Zamora, de la provincia de Buenos Aires, en la que se investigaba una defraudación a través del "phishing". Dicha situación tuvo comienzo cuando personas desconocidas se hicieron con las claves bancarias de la caja de ahorros del Banco Galicia de una persona domiciliada en la ciudad de Buenos Aires, y realizaron una transferencia electrónica a otra cuenta del mismo banco, pero con distinta sucursal, teniendo identificado al titular de la misma.

Luego de encuadrar el delito en la figura de estafa, el magistrado nacional declinó su competencia en favor de la justicia de Monte Grande, donde se hallaba la cuenta desde la cual se extrajo el dinero transferido de forma fraudulenta.

Por su parte, también rechazó la atribución el juzgado local, manifestando que la maniobra de phishing habría sido realizada desde Canadá y que la disposición patrimonial ocurrió fuera de su jurisdicción.

Vuelta al tribunal de origen, su titular mantuvo su postura, dándose por trabada la contienda y elevándose a conocimiento de la corte.

Luego de manifestar que la causa debía resolverse atendiendo a razones de economía procesal y teniendo en cuenta los distintos lugares donde existieron actos con relevancia típica, el Procurador Fiscal declaró:

> En esta inteligencia, atendiendo a que se desconoce el autor o los autores del ataque informático, quienes utilizaron para acceder a internet una conexión, probablemente simulada, en el extranjero (fs. 75/78), entiendo que corresponde al magistrado local continuar con la investigación de la causa, en atención a que en su ámbito territorial se encuentra la cuenta donde se transfirió y se extrajo el dinero (fs. 26 y 91) y se domicilia su titular (fs. 36); quien -por otra parte- también estaría vinculado a un hecho con similares características que investiga la justicia bonaerense (fs. 93, 95 Y 131).

Atentos al dictamen del Procurador, los titulares de la Corte Suprema de Justicia de la Nación declararon competente al Juzgado de Garantías Nº 2 del departamento de justicia de la ciudad de Lomas de Zamora, de la provincia de Buenos Aires.

El segundo[18], resuelto en diciembre, se estableció entre los titulares del Juzgado Nacional en lo Criminal de Instrucción N° 25 y del Juzgado de Instrucción N° 1 de Río Gallegos, provincia de Santa Cruz, a raíz de una denuncia por la venta de pasajes a través de distintas agencias turísticas que actuaban como intermediarias de la firma del denunciante, los cuales eran ofrecidos por el imputado a través de una red social, para lo cual habría sido necesario el ingreso ilegítimo a sus ordenadores desde una dirección de IP de origen extranjero.

Repitiendo la situación de los anteriores fallos, el magistrado nacional rechazó la competencia, alegando que el hecho había ocurrido en la ciudad de Rio Gallegos. Esto debido a que allí se encontraba la entidad bancaria donde fue depositado el dinero adquirido de forma fraudulenta, y donde el titular de la cuenta corriente había realizado dos extracciones.

El juzgado local entendió que la mencionada competencia fue delegada de forma prematura, ya que la realización de los depósitos tanto como el momento en el que fue el perjuicio económico, eran desconocidos.

En el tribunal de origen mantuvo la posición tomada inicialmente, por lo que elevó la causa a la corte.

El Procurador Fiscal expresó que debía resolverse atendiendo a razones de economía procesal y teniendo en cuenta los lugares donde se habrían realizado actos de

[18] Pavón, Cristian Sebastián s/ Estafa. Corte Suprema de Justicia de la Nación, 29 de noviembre de 2016. Recuperado de: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-pavon-cristian-sebastian-estafa-fa16000116-2016-11-29/123456789-611-0006-1ots-eupmocsollaf?q=moreLikeThis%28id-infojus%2C%20numero-norma%5E4%2C%20tipo-documento%5E4%2C%20titulo%5E4%2C%20jurisdiccion%2C%20tesauro%2C%20provincia%2C%20tribunal%2C%20organismo%2C%20autor%2C%20texto%5E0.5%29%3Acompetencia%20estafa&o=5&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal/CORTE%20SUPREMA%20DE%20JUSTICIA%20DE%20LA%20NACION%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Jurisprudencia&t=393 el 10/09/2019.

relevancia típica. Por lo que, sin tener información correspondiente al domicilio e identidad del autor de los hechos realizados desde una conexión, probablemente simulada, desde el extranjero, y teniendo como único elemento cierto que el dinero fue depositado en una cuenta del Banco Patagonia de la ciudad de Rio Gallegos, donde fueron hechas dos extracciones y donde además se domiciliaba el titular, correspondía a la justicia local conocer en la investigación.

La Corte Suprema avaló los fundamentos y conclusiones del Procurador Fiscal, por lo que otorgó la competencia, en este caso, al juzgado local.

Conclusión parcial

Lo desarrollado en este capítulo deja en evidencia que si bien los instrumentos normativos han tratado de dar una solución a los delitos que son cometidos a distancia, los delitos informáticos han traído una modalidad mucho más compleja que las ya conocidas, dejando a los mecanismos de regulación en materia de competencia una considerable dificultad para amoldarse a ellos.

Es importante mencionar que los casos citados en este capítulo son solamente un muestreo general para observar la aplicación de distintos criterios sobre un mismo punto del derecho, que hasta el día de hoy se encuentra en un estado crítico por su incapacidad de determinar la jurisdicción y competencia correspondiente en los casos de delitos informáticos de naturaleza transnacional, con completa certeza y eficacia.

Claramente, el Código Penal Argentino se inclinó por la utilización de la Teoría de la Ubicuidad, atendiendo a los lugares donde se desarrollan inicialmente los hechos, tanto como el lugar donde se manifiestan los resultados de ellos; es decir, todos los lugares donde se hayan desarrollado hechos de relevancia típica.

Sin embargo, muchas veces los ciberdelitos no dejan conocer dichos lugares, dificultando la aplicación de dicha lógica en la práctica, donde realmente estos delitos brindan elementos que no siempre son los mismos y usualmente ostentan una entidad insuficiente, en líneas generales, para determinar con completa claridad el juzgado que debe conocer en las distintas causas que se originen.

Esto produce, como se puede observar en los casos jurisprudenciales citados, un reiterado rechazo de la competencia por parte de los juzgados con jurisdicciones de toda índole, territorialmente hablando. Por lo que se podría considerar que las razones de economía procesal, a las que se hace referencia con mucha frecuencia en los fallos, son justamente las que se vulneran al generarse repetidamente estos conflictos procesales que hacen intervenir a la Corte Suprema de Justicia de la Nación para que produzca resoluciones que aclaren las discordancias.

Para dicho fin, la casuística ha sido la recurrente respuesta y la indiscutible fuente de posteriores controversias, utilizando la ideología de la competencia más favorable, en cuanto a la situación que mejor condición presente en los casos, para ser la que conozca en los casos donde la teoría de la ubicuidad no tenga una respuesta que acoja correctamente la situación de los hechos.

En el ámbito internacional, si bien el Convenio sobre la Ciberdelincuencia de Budapest propone adoptar las medidas necesarias para la fijación de jurisdicción y a realizar consultas en hipotéticas controversias entre estados que reivindiquen su jurisdicción en determinados casos; no hay aún una reglamentación jurídica que sea específica para atribuir la jurisdicción, y mucho menos mecanismos infalibles para resolver los conflictos que se originen.

CONCLUSIONES FINALES

Es innegable la importancia de estos fenómenos actualmente, por la amenaza que representan al elegir como objetivos a los países en vías de desarrollo, situación en la que se encuentra Argentina. Si bien, en líneas generales, los ciberdelitos no son denunciados por las victimas por no tener esperanza en obtener justicia y considerarlo solo una pérdida de tiempo, las estadísticas que se han desarrollado en base a los números que se han podido conocer, demuestran que los delitos informáticos, son un inmenso peligro para los bienes jurídicos protegidos, consistiendo en pérdidas millonarias para personas físicas y jurídicas de todo el mundo.

El phishing, como se ha visto, es la modalidad de estafa realizado en la red a través de la cual se engaña a las víctimas para que ofrezcan información sensible y personal, mediante las cuales los delincuentes sacan provecho de estos datos personales, principalmente, con fines económicos.

Este tipo de delitos, al ser realizados a través de redes informáticas, existen dentro del llamado "ciberespacio" el cual desconoce de fronteras físico-geográficas complicando las investigaciones y persecuciones de estas acciones. Esto es así, debido a que los ordenamientos jurídicos habían instaurado la lógica para determinar las jurisdicciones a través de fronteras basadas en el territorio físico de cada estado, y como se ha desarrollado en este trabajo, este tipo de fenómenos tienen las capacidades de ser transnacionales, con un impacto instantáneo en cuanto al tiempo, y de mantener una distancia abismal entre delincuentes y víctimas, que hacen a estas modalidades delictivas ostentar una importante ventaja ante el derecho actual.

La Argentina después de ciertos conflictos nacionales que atentaban contra la privacidad de correos electrónicos de jueces y periodistas, comenzó una búsqueda de reforma legislativa en materia tecnológica, pero no fue hasta 2008 que esto dio sus frutos. La ley 26.388 trajo consigo una reforma importante para la regulación de los delitos informáticos, sin ser esta una ley específica, sino más bien modificaciones e incorporaciones de figuras delictivas especificas al Código Penal Argentino para reforzar, de alguna manera, a las figuras tradicionales que ya existían en dicho cuerpo normativo, para poder penalizar conductas que, anteriormente a la reforma, recaían en figuras delictivas más leves o, en el peor de los casos, no enmarcando en tipificación alguna.

Si bien la nueva ley subsanó ciertos criterios para enmarcar los delitos, la falta de una reforma procesal penal en este sentido, aun hace que los delitos informáticos sean una tarea ardua para los encargados de sobrellevar los procesos judiciales, ya que principalmente la investigación de estas acciones son complejas por la dificultad creada de recabar material probatorio que ofrezca certeza suficiente del lugar del hecho para determinar la jurisdicción, pero aún más para reconocer el lugar desde el cual actuó el autor del delito.

Es aquí donde se produce el problema central del trabajo, y es la determinación de la competencia judicial. Este es un conflicto histórico del derecho, que como se ha mencionado, se intentó subsanar mediante la determinación de la competencia de delitos tradicionales llevados a cabo a distancia, por parámetros de coordenadas geográficas que establezcan el lugar del hecho de la acción típica, o donde resulte la manifestación de su resultado.

Ante la problemática generada por las características mencionadas de los ciberdelitos, y la falta de una regulación específica que ofrezca claridad a estos temas, la solución que se ha instaurado son las resoluciones que ha otorgado la casuística como fuente para interpretar y fundamentar las contiendas de competencia negativa.

Es difícil considerar correcta la hipótesis planteada al principio de este trabajo, ya que si bien en cierto sentido se cumple lo mencionado, es por partes que así lo hace. Es decir, no hay siquiera en la práctica una única solución que sea predominantemente estable para determinar la jurisdicción y competencia con justeza, siendo utilizado a mi parecer un criterio inclinado a elegir la competencia que sea más conveniente de acuerdo al caso en particular.

Esto hace que se origine una nueva forma de exceptuar a la territorialidad, a través de la aplicación de distintas interpretaciones con una notable flexibilidad de interpretaciones para adoptar la competencia que mejor se amolde. Por lo que es posible que a partir de ello, se produzcan delitos que terminasen impunes a la vez que otros conlleven un exceso de castigo por la expansión del poder punitivo del estado, vulnerando principios y garantías del derecho.

En el ámbito internacional, por otra parte, tampoco se encuentran regulaciones claras acerca de la determinación de competencia en los casos de delitos transnacionales como lo es el phishing, solo el Convenio sobre cibercriminalidad de Budapest ha propuesto que los estados partes que se atribuyan la competencia, concuerden consultas para poder establecer la jurisdicción más adecuada. Sin embargo, de más está decir que es una regla vaga, con poca claridad y carente de precisión.

Concluyendo, a nivel nacional de acuerdo a los fallos estudiados se puede entender que se han resuelto los conflictos mencionando recurrentemente a la economía procesal y a

los lugares donde fueron realizados actos con relevancia típica, pudiendo optar de esta forma en los sitios donde se considera que se realizó el hecho, o donde se manifestó el resultado. En definitiva esto hace expandir el campo de interpretación legislativa para poder optar por la competencia que mejor se ajuste al conflicto en cuestión.

A nivel internacional aún hay mucho trabajo que hacer, pero es importante mantener un rumbo que conlleve a poder conformar en un futuro, un ámbito judicial que abarque a todos los países, o a la gran mayoría en su defecto, procurando crear un campo global y común donde los estados cooperen conjuntamente para combatir este tipo de delitos, teniendo como fin perseguirlos y sancionarlos con la pena que merecen.

Listado de bibliografía

Doctrinarios

- Carlos Julio Lascano (2005) *Derecho penal. Parte general. Libro de estudio.* 1ª ed. Cordoba: Advocatus.
- Fernandez Delpech Horacio (2001) *Internet, su problemática jurídica.* 1ª ed. Buenos Aires: Abeledo Perrot.
- Fernando Miró Llinares (2012) *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.
- G. Balmaceda Hoyos, (2009) *El delito de estafa informática.* Ediciones jurídicas de Santiago.
- Julio Téllez Valdés (2008) *Delitos informáticos.* 4ª ed. Mexico, D.F.: Mc Graw Hill.
- M. Jakobsson, S. Myers (2006) *Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft.* Jhon Wiley & Sons.
- P. G. Lucero y A. A. Kohen. (2011) *Delitos Informáticos.* Versión E-book - 1a ed. - Buenos Aires: Albremática.
- Pablo A. Palazzi (2016) *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388.* 3ª ed. Buenos Aires: Abeledoperrot.
- R. A. Parada y J. D. Errecaborde (2018) *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* - 1a ed . - Ciudad Autónoma de Buenos Aires: Erreius.
- R. Hernández Sampieri, C. Fernández-. Collado y P. Baptista Lucio. (2006) *Metodología de la investigación*. McGraw-Hill. México. 4ª Edición.
- Ruiz Maximiliano (2018) *Ciberterritorialidad: ¿Un nuevo principio de aplicación espacial de la ley penal?.* Recuperado de: https://aldiaargentina.microjuris.com/2018/11/06/ciberterritorialidad-un-nuevo-principio-de-aplicacion-espacial-de-la-ley-penal/ 25/08/2019.
- Torres Neuquen (2008) *Guía de estudio de procesal penal: programa desarrollado de la materia.* 2da ed. Buenos Aires: Estudio.

- Yuni J. y Urbano C. (2014) *Técnicas para investigar: recursos metodológicos para la preparación de proyectos de investigación*.- 1ª ed. - Córdoba: Brujas.

Jurisprudenciales

- Corte Suprema de Justicia de la Nación, "Eden, Alejandro R. s/Denuncia", 18 de octubre de 2016. Recuperado de: https://tuespaciojuridico.com.ar/tudoctrina/2016/12/23/la-csjn-declaro-la-competencia-tribunal-donde-se-encuentra-la-entidad-bancaria-contexto-robo-homebanking/ el 10/09/2019.
- Corte Suprema de Justicia de la Nación, "Jurín Istueta, Aldo Nicolás" - 26/10/2010. SAIJ. Id SAIJ: FA10985852 Recuperado de: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-jurin-istueta-aldo-nicolas-fa10985852-2010-10-26/123456789-258-5890-1ots-eupmocsollaf el 10/09/2019.
- Corte Suprema de Justicia de la Nación, "Pavón, Cristian Sebastián s/estafa", Comp. CCC 66074/2014, 29 de noviembre de 2016. Recuperado de: http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-pavon-cristian-sebastian-estafa-fa16000116-2016-11-29/123456789-611-0006-1ots-eupmocsollaf?q=moreLikeThis%28id-infojus%2C%20numero-norma%5E4%2C%20tipo-documento%5E4%2C%20titulo%5E4%2C%20jurisdiccion%2C%20tesauro%2C%20provincia%2C%20tribunal%2C%20organismo%2C%20autor%2C%20texto%5E0.5%29%3Acompetencia%20estafa&o=5&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal/CORTE%20SUPREMA%20DE%20JUSTICIA%20DE%20LA%20NACION%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Jurisprudencia&t=393 el 10/09/2019.
- Corte Suprema de Justicia de la Nación, "Piccadaci, José Guillermo s/estafa", Comp. CCC 60569/2015, 20 de diciembre de 2016.

Legislativos

- Código Penal de la Nación Argentina.
- Convenio de Budapest sobre Ciberdelito.
- Ley 26.388 de Ley de Delitos Informáticos.
- Ley 27.411. Aprobación del Convenio sobre Ciberdelito (Convenio de Budapest sobre Ciberdelito)